SPYWOLF

Security Audit Report

Completed on

May 26, 2023

SPYWOLF.CO
@SPYWOLFNETWORK
@SPYWOLFNETWORK

OVERVIEW

This audit has been prepared for **RC Launchpad** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

TABLE OF CONTENTS

RC Launchpad

PROJECT DESCRIPTION

According to their whitepaper:

RC LAUNCHPAD is a blockchain platform designed to provide an easy to use launchpad that aims to help new quality blockchain projects to raise capital and easily distribute their tokens at the same time. RC LAUNCHPAD currently operates on the Binance Smart Chain and helps launch the new IDO coins via a Decentralized liquidity Exchange(DEX) such as PancakeSwap.

Release Date: Presale starts in July, 2023

Category: Launchpad

CONTRACT INFO

Token Name
RCSALE Launchpad

Symbol
RCS

Contract Address
0xbCCbDe7D0EC34676a337D395f2cbB5FA2a82dDBd

Network
Binance Smart Chain

Language
Solidity

Deployment Date
Sep 25, 2022

Verified?
Yes

Total Supply
5,000,000,000

Status
Not launched

TAXES

Buy Tax
3%

Sell Tax
10%

*Taxes can be changed in future

Our Contract Review Process

The contract review process pays special attention to the following:

- Testing the smart contracts against both common and uncommon vulnerabilities
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

TOKEN TRANSFERS STATS

Transfer Count	2
Uniq Senders	2
Uniq Receivers	2
Total Amount	9043750000 RCS
Median Transfer Amount	5000000000 RCS
Average Transfer Amount	4521875000 RCS
First transfer date	2022-09-25
Last transfer date	2023-05-20
Days token transferred	2

SMART CONTRACT STATS

Calls Count	11
External calls	7
Internal calls	4
Transactions count	8
Uniq Callers	2
Days contract called	1
Last transaction time	2023-05-20 01:19:18 UTC
Created	Sep-25-2022 08:46:14 PM +UTC
Create TX	0x5a6641670e164e8845e1deda19bad8ce62d58e6e32cc8b834e0ee65029d9dca1
Creator	0x39bb0e2fdc2dc86f76c2c1fe9e54744defcff0e7

VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

FOUND THREATS

⚠ High Risk

Update fees function does not actually update the fees but leave them unchanged.
Fees state variables should be equal to the new input values instead of current state variable ones.
Checks should be performed on the input values instead on state variable values.

```
function updateFees(
    uint256 _marketingBuyFee, uint256 _marketingSellFee, uint256 _liquidityBuyFee,
    uint256 _liquiditySellFee, uint256 _rewardsBuyFee, uint256 _rewardsSellFee
) public onlyOwner {
    require(
        rewardsBuyFee.add(liquidityBuyFee).add(marketingBuyFee) <= 30,
        "Buy total fee cannot be greater than 30%"
    );
    require(
        rewardsSellFee.add(liquiditySellFee).add(marketingSellFee) <= 30,
        "Sell total fee cannot be greater than 30%"
    );

    marketingBuyFee = marketingBuyFee;
    marketingSellFee = marketingSellFee;
    liquidityBuyFee = liquidityBuyFee;
    liquiditySellFee = liquiditySellFee;
    rewardsBuyFee = rewardsBuyFee;
    rewardsSellFee = rewardsSellFee;

    totalBuyFees = rewardsBuyFee.add(liquidityBuyFee).add(marketingBuyFee);
    totalSellFees = rewardsSellFee.add(liquiditySellFee).add(
        marketingSellFee
    );

    emit UpdateFees(
        _marketingBuyFee, _marketingSellFee, _liquidityBuyFee,
        _liquiditySellFee, _rewardsBuyFee, _rewardsSellFee
    );
}
```

- Recommendation:
  - Considered as good tax deduction practice is buy and sell fees combined not to exceed 25%.

FOUND THREATS

⚠ High Risk

Owner can set max sell transaction limit without limitations, if set to 0, users won't be able to sell.

```
function updateMaxAmount(uint256 newNum) public onlyOwner {
    require(maxSellTransactionAmount != newNum);
    maxSellTransactionAmount = newNum * (10**9);
}

function _transfer(
    address from,
    address to,
    uint256 amount
) internal override {
.....................
if (
    !swapping &&
    tradingEnabled &&
    automatedMarketMakerPairs[to] && // sells only by detecting transfer to automated market maker pair
    from != address(uniswapV2Router) && //router -> pair is removing liquidity which shouldn't have max
    !_isExcludedFromFees[to] && //no max for those excluded from fees
    maxSellTransactionAmount != 0 // if 0 means disabled
) {
    require(
        amount <= maxSellTransactionAmount,
        "Sell transfer amount exceeds the maxSellTransactionAmount."
    );
}
.....................
}
```

- Recommendation:
  - Considered as good transaction limit practice is transaction limits to be always equal or above 0.1% of total supply.

FOUND THREATS

⚠ Medium Risk

Owner can change auto swap settings.
If swapTokensAtAmount is set to 0 and contract token balances are 0, contract will halt and selling will fail.

```
function updateSwapTokensAtAmount(uint256 newAmountToSwap) public onlyOwner {
    swapTokensAtAmount = newAmountToSwap;
}

function _transfer(
    address from,
    address to,
    uint256 amount
) internal override {
.....................
uint256 contractTokenBalance = balanceOf(address(this));

bool canSwap = contractTokenBalance >= swapTokensAtAmount;

if (
    tradingEnabled &&
    canSwap &&
    !swapping &&
    !automatedMarketMakerPairs[from] &&
    from != liquidityWallet &&
    to != liquidityWallet &&
    swapAndLiquifyEnabled
) {
    swapping = true;

    uint256 totalBuySell = buyAmount.add(sellAmount);

    uint256 swapAmountBought = contractTokenBalance.mul(buyAmount).div(
        totalBuySell
    );
    uint256 swapAmountSold = contractTokenBalance.mul(sellAmount).div(
        totalBuySell
    );
.....................
}
```

- Recommendation:
  - Ensure that swapTokensAtAmount's value is always above 1 token (consider token decimals).

Informational

Staked user cannot sell their tokens before the stake ending period.

```
function stake(uint256 duration) public {
.....................
stakingUntilDate[_msgSender()] = block.timestamp.add(duration);
.....................
}

function _transfer(
    address from,
    address to,
    uint256 amount
) internal override {
.....................

if (!automatedMarketMakerPairs[from] && stakingEnabled) {
    require(
        stakingUntilDate[from] <= block.timestamp,
        "Tokens are staked and locked!"
    );
    if (stakingUntilDate[from] != 0) {
        stakingUntilDate[from] = 0;
        stakingBonus[from] = 0;
        try dividendTracker.setBalance(payable(from), 0) {} catch {}
        emit StakeExit(from, block.timestamp);
    }
}
.....................
}
```

Informational

Owner can exclude address from fees.
When address is excluded from fees, the user will receive the whole amount of the bought, sold and/or transferred tokens.

```
function excludeFromFees(address account, bool excluded) public onlyOwner {
    require(_isExcludedFromFees[account] != excluded);
    _isExcludedFromFees[account] = excluded;

    emit ExcludeFromFees(account, excluded);
}
```

Owner can enable/disable staking.

```
function enableStaking(bool enable) public onlyOwner {
    require(stakingEnabled != enable);
    stakingEnabled = enable;

    emit EnableStaking(enable);
}
```

Informational

Owner can change staking rewards multiplier for each staking duration up to 500 for duration period.

```
function updateStakingAmounts(uint256 duration, uint256 bonus)
    public
    onlyOwner
{
    require(stakingAmounts[duration] != bonus);
    require(bonus <= 500, "Staking bonus can't exceed 500%");

    stakingAmounts[duration] = bonus;
    emit UpdateStakingAmounts(duration, bonus);
}

function stake(uint256 duration) public {
    require(stakingEnabled, "Staking is not enabled");
    require(stakingAmounts[duration] != 0, "Invalid staking duration");
    require(
        stakingUntilDate[_msgSender()] < block.timestamp.add(duration),
        "already staked for a longer duration"
    );

    stakingBonus[_msgSender()] = stakingAmounts[duration];
    stakingUntilDate[_msgSender()] = block.timestamp.add(duration);

    uint256 stakingBalanceToSet = balanceOf(_msgSender())
        .mul(stakingAmounts[duration].add(100))
        .div(100);

    dividendTracker.setBalance(_msgSender(), stakingBalanceToSet);

    emit StakeEnter(
        _msgSender(),
        duration,
        block.timestamp,
        block.timestamp + duration
    );
}
```

RECOMMENDATIONS FOR

GOOD PRACTICES

1. Consider fundamental tradeoffs
2. Be attentive to blockchain properties
3. Ensure careful rollouts
4. Keep contracts simple
5. Stay up to date and track development

RC Launchpad

GOOD PRACTICES FOUND

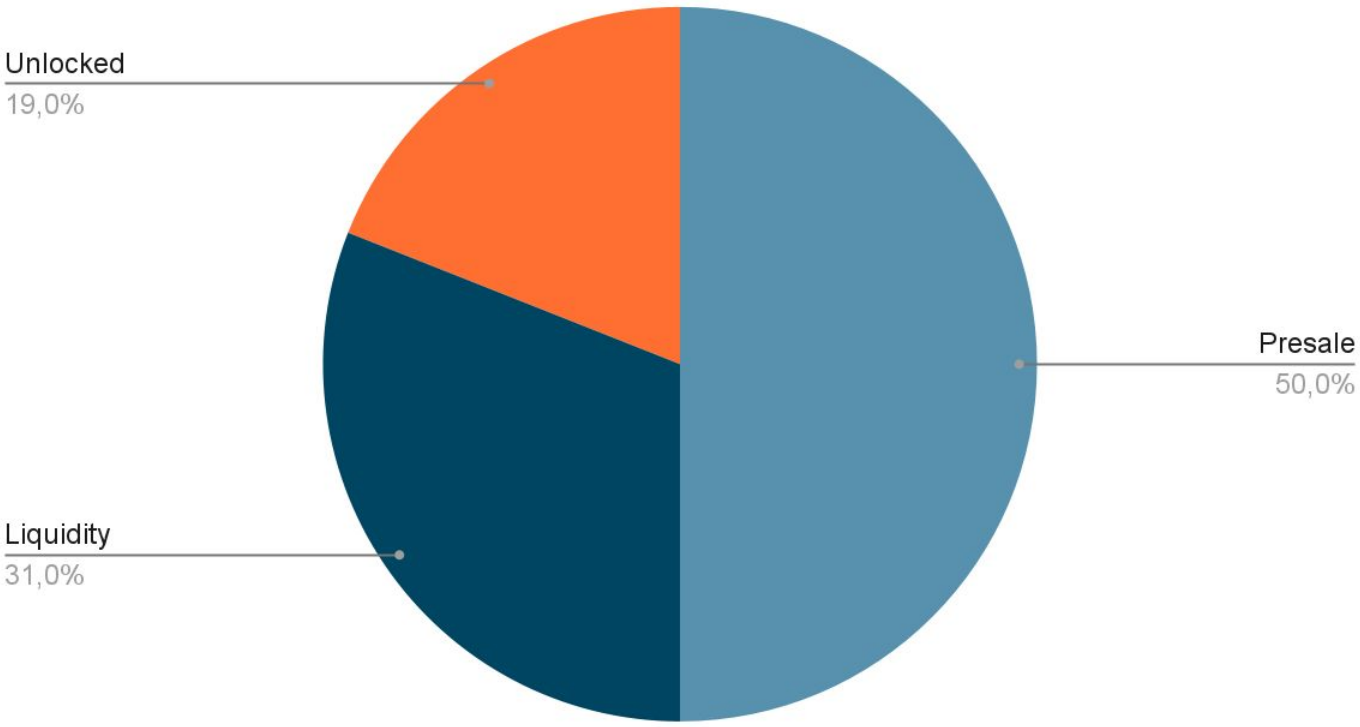
- ✔ The owner cannot mint new tokens after deployment
- ✔ The smart contract utilizes "SafeMath" to prevent overflows

TOKENOMICS

The following tokenomics are based on Pinksale's presale page:

- 50% - Presale
- 31% - Liquidity
- 19% - Unlocked

Tokens distribution



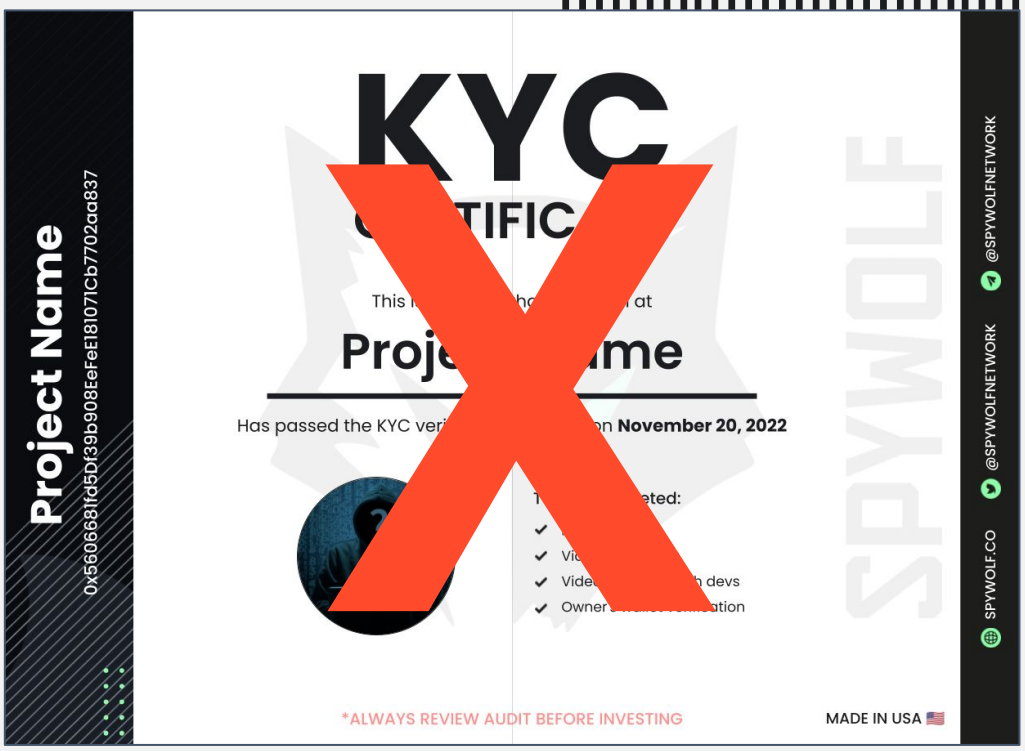
THE TEAM

⚠️ The team is annonymous

KYC INFORMATION

⚠️ No KYC

We recommend the team to get a KYC in order to ensure trust and transparency within the community.



WEBSITE

Website URL
https://rcsale.app/

Domain Registry
https://www.godaddy.com

Domain Expiration
2023-12-16

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

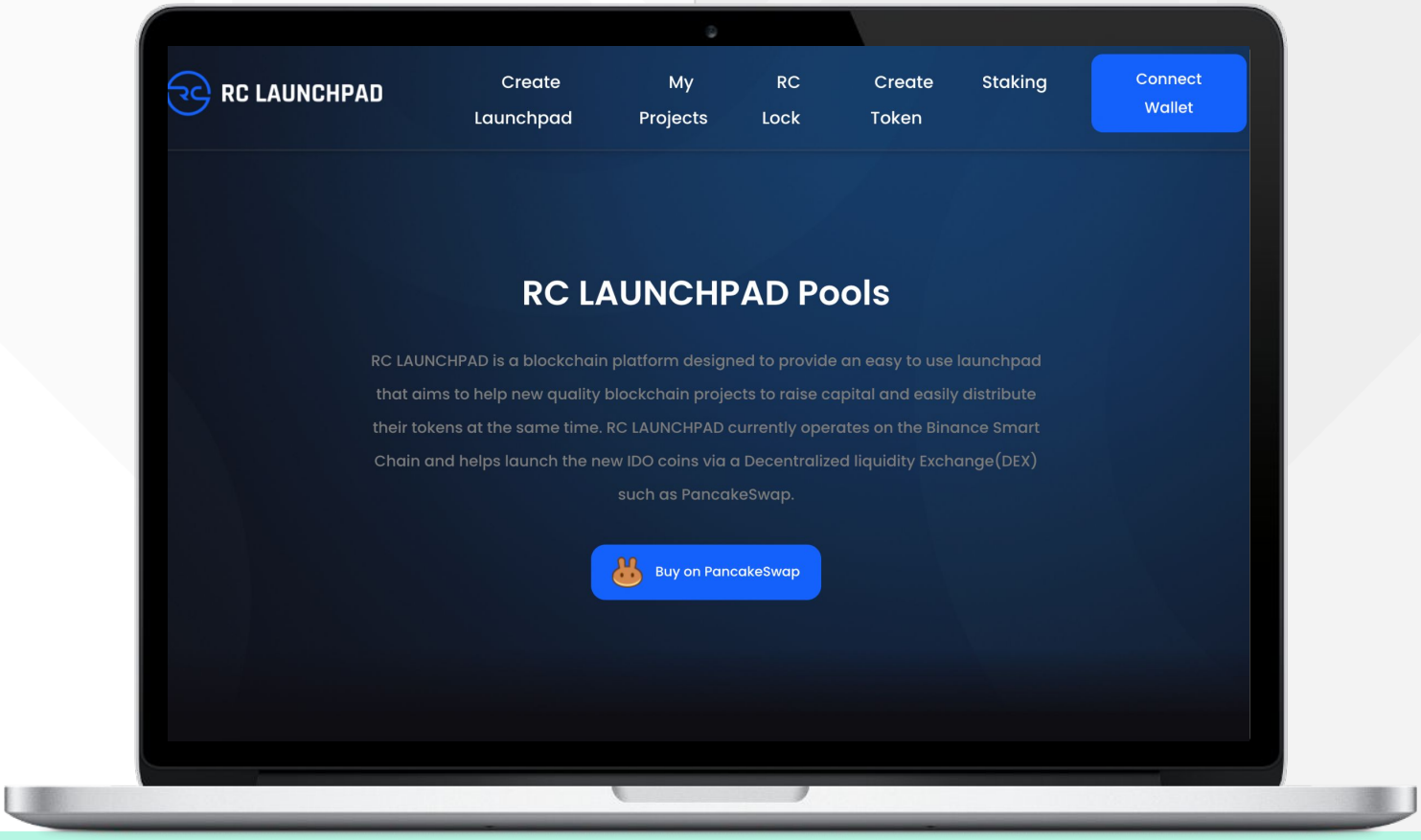
Design
Single page design with appropriate color scheme and graphics.

Content
The information helps new investors understand what the product does right away. No grammar mistakes found.

Whitepaper
Well written but a bit short

Roadmap
Yes

Mobile-friendly?
Yes



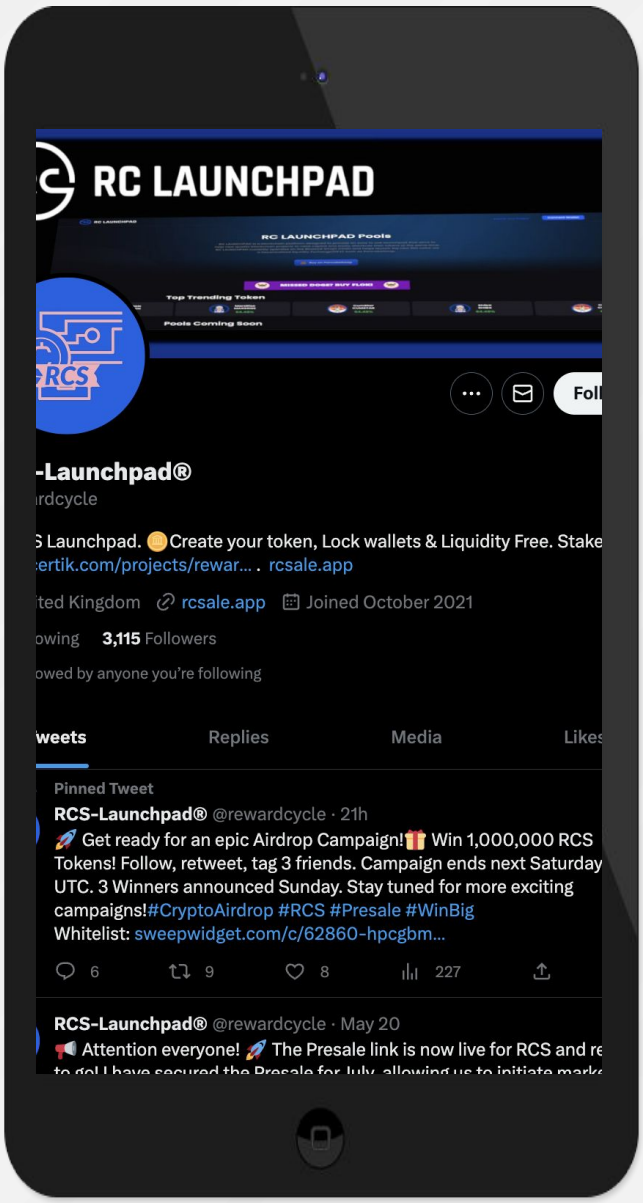
rcsale.app

SOCIAL MEDIA

& ONLINE PRESENCE

ANALYSIS

Social media pages are active.



Twitter

@rewardcycle

- 3155 followers
- Active

Discord

- Not available

Telegram

@TelegramUSERNAME

- 2613 members
- Active members
- Active mods

Medium

- Not available

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- **OVER 500 SUCCESSFUL CLIENTS**
- **MORE THAN 500 SCAMS EXPOSED**
- **MILLIONS SAVED IN POTENTIAL FRAUD**
- **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**
- **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE

SPYWOLF.CO

@SPYWOLFNETWORK

@SPYWOLFNETWORK

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.
While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:
By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.
No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.
The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.
No applications were reviewed for security. No product code has been reviewed.